Notice of Allowability	Application No.	Applicant(s)	
	09/739,260	SANDHU ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *The After-Final Amendment received 31 May 2005*.

2. ☒ The allowed claim(s) is/are *1-16 and 18-31*.

3. ☒ The drawings filed on *14 January 2005* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

EXAMINER'S AMENDMENT

1. The Amendment after Final rejection received 31 May 2005 has been entered and made of record in the present application.

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Alfred Stadnicki on 14 June 2005.

The application has been amended as follows:

REPLACE the claims with the following complete listing of claims.

The following listing of claims will replace all prior versions and listings of claims in the present application:

Claim 1 (Original) A system for generating an asymmetric crypto-key usable to transform messages to encrypt and decrypt or sign the messages for a user, comprising:

a first processor configured to (i) generate a private crypto-key and a corresponding public crypto-key associated with the user, (ii) divide the private crypto-key into a first private key portion, based on a password of the user, and a second private key portion, (iii) destroy the private crypto-key and the first private key portion without distribution thereof and without storage thereof in a persistent state, and (iv) store only the second private key portion and the public crypto-key in a persistent state; and

a second processor representing a user and configured to (i) generate, responsive to receipt of an inputting of and based on the user password, only the first private key portion, and (ii) destroy, without storing in a persistent state, the generated first private key portion.

Claim 2 (Original) A system according to claim 1, wherein the user password has a bit length of between 56 and 72 bits and the generated first private key portion has a bit length of at least 257 bits.

Claim 3 (Original) A system according to claim 1, wherein the first private key portion is generated in accordance with a one way function.

Claim 4 (Original) A system according to claim 3, wherein:

the first processor and the second processor are further configured to selectively operate in a first mode and a second mode;

in the first mode the first processor and the second processor apply the one way function a first number of times to generate the first private key portion; and

in the second mode the first processor and the second processor apply the one way function a second number of times, different than the first number of times, to generate the first private key portion.

Claim 5 (Original) A system according to claim 4, wherein:

the first processor and the second processor are further configured to select one of the first and second mode for operation based on at least one of an identity of the user and a strength of the user password.

Claim 6 (Original) A system according to claim 3, wherein:

the first processor and the second processor are further configured to select the one way function from a group of one way functions.

Claim 7 (Original) A system according to claim 6, wherein:

the first processor and the second processor are further configured to select the one way function based upon at least one of an identity of the user and a strength of the user password.

Claim 8 (Original) A system according to claim 1, wherein:

the second processor is further configured to encrypt or sign a message with the first private key portion prior to destroying the generated first private key portion; and

the first processor is further configured to recover or verify the encrypted message by applying the stored second private key portion and the public key.

Claim 9 (Original) A system for asymmetrically transforming a message, comprising:

a first processor representing a user and configured to generate, based on a password of the user, a first portion of a private crypto-key, to transform a message with the first private key portion, and to destroy the generated private key portion after transforming the message and;

a second processor configured to further transform the transformed message by applying at least one of a second portion of the private crypto-key and a public crypto-key, both of which correspond to the first private key portion.

Claim 10 (Original) A system according to claim 9, further comprising:

a storage device configured to store the second private key portion and the public crypto-key in a persistent state;

wherein the applied at least one of a second portion of the private crypto-key and a public crypto-key is at least one of the stored second private key portion and the stored public crypto-key, and the second processor is further configured to retrieve the at least one of the stored second private key portion and the stored public crypto-key based on the user password;

wherein the first private key portion is never stored in a persistent state.

Claim 11 (Original) A system according to claim 9, wherein the user password has a bit length of between 56 and 72 bits and the generated first private key portion has a bit length of at least 257 bits.

Claim 12 (Original) A system according to claim 9, wherein the first private key portion is generated in accordance with a one way function.

Claim 13 (Original): A system according to claim 12, wherein:

the first processor and the second processor are further configured to selectively operate in a first mode and a second mode;

in the first mode the first processor and the second processor apply the one way function a first number of times to generate the first private key portion; and

in the second mode the first processor and the second processor apply the one way function a second number of times, different than the first number of times, to generate the first private key portion.

Claim 14 (Previously Presented) A system according to claim 13, wherein:

the first processor and the second processor are further configured to select one of the first and second mode for operation based on at least one of an identity of the user and a strength of the user password.

Claim 15 (Original) A system according to claim 12, wherein:

the first processor and the second processor are further configured to select the one way function from a group of one way functions.

Claim 16 (Original) A system according to claim 15, wherein:

the first processor and the second processor are further configured to select the one way function based upon at least one of an identity of the user and a strength of the user password

Claim 17 (Cancelled)

Claim 18 (Original) A method for generating an asymmetric crypto-key usable to transform messages to both encrypt and decrypt the messages for a user, comprising:

generating, based upon a password of the user, a private crypto-key and a corresponding public crypto-key associated with the user;

dividing the private crypto-key into a first private key portion and a second private key portion;

destroying the private crypto-key and the first private key portion without distribution thereof and without storage thereof in a persistent state;

separately generating, responsive to receipt of, and based upon, the user password, only the first private key portion; and

destroying, without storing in a persistent state, the separately generated first private key portion.

Claim 19 (Original) The method according to claim 18, wherein the password has a bit length of 56 to 72 bits and the generated first private key portion has a bit length of at least 257 bits.

Claim 20 (Original) The method according to claim 18, wherein the first private key portion is generated in accordance with a one way function.

Claim 21 (Original) The method according to claim 18, further comprising:

selecting one of a first mode and a second mode in which to generate the first private key portion in accordance with a one way function;

wherein the first mode the one way function is applied to the password a first number of times to generate the first private key portion; and

wherein the second mode the one way function is applied to the password a second number of times, different than the first number of times, to generate the first private key portion.

Claim 22 (Original) The method according to claim 21, wherein selection of the first and second mode is based on at least one of an identity of the user and a strength of the user password.

Claim 23 (Original) The method according to claim 18, further comprising:

selecting a one way function from a group of one way functions; and

generating the first private key portion in accordance with the selected one way function;

wherein selection of the one way function is based upon at least one of an identity of the user and a strength of the user password.

Claim 24 (Original) The method according to claim 18, further comprising:

transforming a message with the generated first private key portion prior to destruction thereof; and

further transforming the message by applying at least one of the second private key portion and the public crypto-key.

Claim 25 (Original) The method according to claim 24, further comprising:

storing the second private key portion and the public crypto-key in a persistent state; and

retrieving the at least one of the stored second private key portion and the stored public crypto-key;

wherein the applied at least one of the second private key portion and the public crypto-key is at least one of the retrieved at least one of the second private key portion and the public crypto-key; and

wherein the first private key portion is never stored in a persistent state.

Claim 26 (Currently Amended) A method for ~~communicating a transformed~~transforming a message, in which a user is associated with a private crypto-key and a corresponding public crypto-key, and the private crypto-key has a first private key portion and a second private key portion, comprising:

processing a password to generate the first private key portion and transforming a first message with the generated first private key portion; and

further transforming the first message with the second private portion;

wherein the first private portion is (i) not persistently stored at any networked device and (ii) not transmitted over a network;

wherein the processing and transforming are performed by a networked device representing the user, and the further transforming is performed by a networked device representing other than the user.

Claim 27 (Previously Presented) The method according to claim 26, wherein the password has a bit length of 56 to 72 bits and the generated first private key portion has a bit length of at least 257 bits.

Claim 28 (Original) The method according to claim 27, wherein the first private key portion is generated in accordance with a one way function.

Claim 29 (Original) The method according to claim 27, further comprising:

selecting one of a first mode and a second mode in which to generate the first private key portion in accordance with a one way function;

wherein the first mode the one way function is applied to the password a first number of times to generate the first private key portion; and

wherein the second mode the one way function is applied to the password a second number of times, different than the first number of times, to generate the first private key portion.

Claim 30 (Original) The method according to claim 29, wherein selection of the first and second mode is based on at least one of an identity of the user and a strength of the user password.

Claim 31 (Original) The method according to claim 27, further comprising:

selecting a one way function from a group of one way functions; and

generating the first private key portion in accordance with the selected one way function;

wherein selection of the one way function is based upon at least one of an identity of the user and a strength of the user password.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER